БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

**Тестирование генераторов псевдослучайных
последовательностей на основе цепей Маркова
переменной длины**

Воробьева Мария Игоревна

Научный руководитель – кандидат физ.-мат. наук, доцент кафедры ММАД

М.В. Мальцев

Минск, 2020

РЕФЕРАТ

Дипломная работа, 58 с., 6 рис., 6 табл., 19 источников, 1 приложение.

ТЕСТИРОВАНИЕ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ЦЕПЕЙ МАРКОВА ПЕРЕМЕННОЙ ДЛИНЫ.

Объект исследования — криптографические генераторы, марковские модели.

Цель работы — тестирование генераторов псевдослучайных последовательностей и выявление зависимостей, разработка алгоритма тестирования на основе цепи Маркова переменной длины .

Методы исследования — использование статистических методов для анализа выходных последовательностей, методы теории вероятностей и математической статистики.

Результат — реализован алгоритм статистического тестирования последовательностей чисел на основе марковской цепи переменной длины, получены численные результаты компьютерных экспериментов.

ABSTRACT

Thesis, 58 p., 6 fig., 6 tab., 19 s., 1 appendix.

TESTING PSEUDORANDOM SEQUENCE GENERATORS BASED ON VARIABLE LENGTH MARKOV CHAINS.

The object of the study is Cryptographic generators, Markov models.

The aim of the work is testing pseudorandom sequence generators and identifying dependencies, developing a testing algorithm based on a variable length Markov chain.

The methods of investigation are the use of statistical methods for analyzing output sequences, methods of probability theory and mathematical statistics.

The result is an algorithm for statistical testing of cryptographic generators based on a Markov chain of variable length, and numerical results of computer experiments are obtained.